CNS 1/2020

Opinion regarding the consultation of a clinical analysis laboratory, in relation to the consideration of the person in charge or responsible regarding the performance and conservation of analyzes

A letter from the data protection officer of a laboratory that performs clinical analyzes is presented to the Catalan Data Protection Authority, in which he explains that several hospitals subcontract this laboratory to carry out analytical tests on admitted patients. The consultation adds that the laboratory has no contact with the patient and that as a laboratory they are subject to the conservation of health data.

Taking this into account, the inquiry asks whether the laboratory can be considered responsible for the processing of the analysis or whether they will always necessarily be responsible.

Having analyzed the request, given the applicable regulations and the report of the Legal Counsel, the following is ruled.

I

(...)

II

The inquiry states that the clinical analysis laboratory works with different hospitals, both public and private, which subcontract the laboratory to perform analyzes on their admitted patients.

According to the inquiry, in order to perform this service, the hospitals communicate to the laboratory the identification data of the affected patients and send them the samples taken from them by the hospital's health professionals, so that the laboratory can analyze them and return them electronically or in paper the personalized results report for each patient, without the laboratory having any contact with the patients.

The consultation adds that as a laboratory they are subject to Law 41/2002, of November 14, basic regulation of patient autonomy and rights and obligations in terms of information and clinical documentation, "which obliges them to keep the documentation for a minimum period of 15 years in Catalonia."

With all this, the query asks the following question:

"Considering that the laboratory has no contact with the interested party of the data (patients), and that on the other hand regardless of the instructions we may receive from the hospital they are obliged to keep the health data, we request a report from the Authority setting out whether (the laboratory) can be considered in charge of this treatment of the performance of analyzes or will they always necessarily be responsible?"

Based on the consultation in these terms, we agree that the legal regime applicable to the protection of personal data is Regulation (EU) 2016/679, of April 27, general data protection (RGPD).

It is also necessary to take into account the provisions of Organic Law 3/2018, of December 5, on the protection of personal data and the guarantee of digital rights (LOPDGDD).

The processing of personal data (art. 4.1 RGPD) of natural persons who are admitted to hospitals and who receive health care, specifically, patients in hospitals where clinical analyzes are carried out that will later be sent to the laboratory who formulates the query, is subject to the principles and guarantees of the personal data protection regulations, in particular, the RGPD and the LOPDGDD.

III

It is responsible for data processing: "the natural or legal person, public authority, service or other organism that, alone or together with others, determines the purposes and means of the treatment; if the Law of the Union or of the Member States determines the purposes and means of the treatment, the person responsible for the treatment or the specific criteria for his appointment may be established by the Law of the Union or of the Member Sta (art. 4.7 RGPD).

It is responsible for the treatment: "the natural or legal person, public authority, service or other organism that treats personal data on behalf of the person responsible for the treatment;" (art. 4.8 GDPR).

From the perspective of data protection, we start from the basis that the processing of personal data subject to consultation must have a person in charge, who consequently assumes a series of responsibilities and obligations regarding the processing that is carried out.

It is necessary to take into account the provisions of Law 21/2000, of 29 December, on the rights of information concerning the patient's health and autonomy, and clinical documentation.

According to article 9.1 of Law 21/2000:

> "1. The clinical history collects the set of documents relating to the healthcare process of each patient while identifying the doctors and other healthcare professionals who have intervened. The maximum possible integration of each patient's clinical documentation must be sought. This integration must be done, at least, in the scope of each center, where there must be a unique clinical history for each patient."

In the same sense, article 14.1 of Law 41/2002, basic, of November 14, on patient autonomy.

We start from the basis that each health center, such as the hospitals referred to in the query, is responsible for the treatment of the clinical history data (hereafter, HC) of its patients who are admitted or treated there.

The outsourcing of a certain service by a person in charge can be understood as a management instrument that consists of the contracting by the hospitals (as responsible for the data of the patients who are admitted there), of a third party (the laboratory that formulates the consultation), for the performance of a certain service, in particular, the analysis and obtaining results of the samples of certain patients, which the hospital itself sends to it together with the identifying data of these .

Outsourcing of this service by hospitals is a decision of each hospital.

It is the hospital, as responsible for the clinical history of its patients, that can decide that the data of certain patients are processed by the laboratory, as a third party external to the hospital itself, or perform the analytical tests through its own services .

It would be a different matter if the laboratory did not act on behalf of a hospital based on the subcontracting of a service, but on its own account, for example, regarding the processing of the personal data of a person who addresses it directly for take an analytical test that the laboratory offers as its own service.

However, based on the information available, this is not the assumption being made.

For all that has been said, given the information provided, when a hospital subcontracts the analysis of its patients to the laboratory, and the laboratory has to process personal data of these patients, there can be no doubt that the hospital is the responsible, since he is the one who decides that this laboratory is the one that does the analysis, which analytical tests need to be performed on certain patients, and communicates the necessary information to the laboratory (identifying data and patient samples).

Therefore, it is clear that it is the hospital that "determines the purposes and treatment" of the patients' data, and that the laboratory is in charge of the treatment of this data on behalf of the hospital. In fact, the consultation itself explains that the laboratory "receives instructions" from the health center in relation to the performance of analytical tests.

In this sense, the treatment order must be governed by the provisions of article 28 of the RGPD, according to which:

> "1. When a treatment is to be carried out on behalf of a person responsible for the treatment, he will only choose a person in charge who offers sufficient guarantees to apply appropriate technical and organizational measures, so that the treatment complies with the requirements of this Regulation and guarantees the protection of the rights of the interested party.
>
> 2. The person in charge of the treatment will not resort to another person in charge without the prior written authorization, specific or general, of the person in charge. In this last case, the person in charge will inform the person in charge of any change envisaged in the incorporation or substitution of other persons in charge, thus giving the person in charge the opportunity to oppose said changes.
>
> 3. The treatment by the controller will be governed by a contract or other legal act in accordance with the Law of the Union or the Member States, which binds the controller with respect to the controller and establishes the object, duration, nature and purpose of the treatment, the type of personal data and categories of interested parties, and the obligations and rights of the person in charge. Said contract or legal act will stipulate, in particular, that the manager:
>
> a) will treat personal data solely following the documented instructions of the person in charge, including with respect to the transfer of personal data to a third country or an international organization, unless it is obliged to do so by virtue of the Law of the Union or of the Member States that applies to the person in charge; in such a case, the manager will inform the person in charge of that legal requirement prior to the treatment, unless such Law prohibits it for important reasons of public interest;

b) will guarantee that the persons authorized to treat personal data have committed to respect confidentiality or are subject to a confidentiality obligation of a statutory nature;

c) will take all the necessary measures in accordance with article 32;

d) will respect the conditions indicated in sections 2 and 4 to resort to another treatment manager;

e) will assist the person in charge, taking into account the nature of the treatment, through appropriate technical and organizational measures, whenever possible, so that he can comply with his obligation to respond to requests aimed at the exercise of the rights of the interested parties established in chapter III;

f) will help the manager to ensure compliance with the obligations established in articles 32 to 36, taking into account the nature of the treatment and the information available to the manager;

g) at the choice of the person responsible, will delete or return all personal data once the provision of the treatment services is finished, and will delete the existing copies unless the conservation of personal data is required under Union Law or member states;

h) will make available to the person in charge all the information necessary to demonstrate compliance with the obligations established in this article, as well as to allow and contribute to the performance of audits, including inspections, by the person in charge or another auditor authorized by said responsible

In relation to what is provided in letter h) of the first paragraph, the person in charge will immediately inform the person in charge if, in his opinion, an instruction infringes the present Regulation or other provisions in the area of data protection of the Union or the Member States. "

Likewise, according to article 33.1 of the LOPDGDD:

"1. The access by a data controller to personal data that is necessary for the provision of a service to the controller will not be considered data communication as long as it complies with the provisions of Regulation (EU) 2016/679, in this law organic and in its development standards.

In addition, when it comes to assignments subject to Law 9/2017, of November 8, on public sector contracts (LCSP), it must be taken into account that, according to article 122.2 LCSP:

"2. The solvency criteria and award of the contract will be included in the particular administrative clauses; the social, labor and environmental considerations that are established as solvency, award criteria or as special conditions of execution; the agreements and conditions defining the rights and obligations of the parties to the contract; the provision of assignment of the contract except in cases where it is not possible in accordance with what is established in the second paragraph of article 214.1; the obligation of the awardee to comply with the salary conditions of the workers in accordance with the applicable sectoral Collective Agreement; and the other mentions required by this Law and its implementing rules. In the case of mixed contracts, the regime will be detailed

legal applicable to its effects, fulfillment and termination, in accordance with the rules applicable to the different benefits merged into them.

The documents may also specify whether the transfer of intellectual or industrial property rights will be required, without prejudice to the provisions of article 308 regarding service contracts.

The documents must expressly mention the obligation of the future contractor to respect the current regulations on data protection.

Without prejudice to the provisions of article 28.2 of Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016, relating to the protection of individuals with regard to the processing of personal data and the free circulation of these data and for which Directive 95/46/CE is repealed, in those contracts whose execution requires the processing of personal data by the contractor on behalf of the person in charge of the processing, the application will additionally state:

a) The purpose for which said data will be transferred.
b) The obligation of the future contractor to submit in any case to the national and European Union regulations on data protection, without prejudice to what is established in the last paragraph of section 1 of article 202. c) The obligation of the awarded company to present before the formalization of the contract a declaration in which it makes clear where the servers will be located and from where the services associated with them will be provided. d) The obligation to communicate any change that occurs, throughout the life of the contract, of the information provided in the statement referred to in letter c) above. e) The obligation of the bidders to indicate in their offer, if they intend to subcontract the servers or the services associated with them, the number or the business profile, defined by reference to the conditions of professional or technical solvency, of the subcontractors to those that are going to be entrusted with their implementation.

In the documents corresponding to the contracts referred to in the previous paragraph, the obligations listed in letters a) and e) above must in any case be qualified as essential for the purposes of what is provided for in letter f) of section 1 of article 211 .”

In other words, it is necessary for each hospital, as responsible for the HC of its patients, to establish the corresponding treatment contract in order to be able to process the data of the patients on whom analytical tests need to be performed, in the terms provided for in the Article 28 of the RGPD.

IV

According to the consultation, "regardless of the instructions we might receive from the hospital", the laboratory would be obliged to keep the data, since they are subject to Law 41/2002, which obliges them to keep the documentation for a minimum period of 15 years in Catalonia.

It seems that the consultation would link the necessary conservation of information by the laboratory, to the doubt expressed about its role as responsible or in charge.

Effectively, the patient autonomy regulations provide for certain retention periods for the patients' HC documentation, content that is specified in article 10.1 of Law 21/2000 (patient identification data and assistance, clinical care data and social data):

Article 12 of Law 21/2000 regulates the conservation of the HC in the following terms:

> **"1. The responsibility for guarding the clinical history rests with the management of the health centers, or with the health professionals who carry out their activity individually.**
>
> **(...)**
>
> **4. The following documentation must be kept from the clinical history, together with the identification data of each patient, for at least fifteen years from the date of discharge of each care process: a) The sheets of informed consent. b) The discharge reports. c) Surgical reports and birth registration. d) Data relating to anesthesia. e) The reports of complementary explorations. f) The necropsy reports. g) Pathological anatomy reports.**
>
> **(...)**
>
> **6. The documentation that makes up the clinical history not mentioned in section 4 can be destroyed once five years have passed from the date of registration of each care process.**
>
> **(...)**
>
> **8. The decision to keep the clinical history, in the terms established by section 7, corresponds to the medical management of the health center, at the proposal of the doctor, with the prior report of the unit in charge of managing the clinical history in each center. This decision corresponds to the doctors themselves when they carry out their activity individually.**
>
> **(...).”**

Thus, it is clear that the patient autonomy regulations establish the conservation of certain information for different periods of time, not necessarily 15 years.

For the purposes that are relevant, it should be borne in mind that when a person in charge decides to establish a processing order, which would be the case in question given the information available, one of the issues that must be determined in the contract is the destination of the data at the end the benefit

Article 28.3 of the RGPD, section g), provides the following:

g) at the choice of the person responsible, will delete or return all personal data once the provision of the treatment services is finished, and will delete the existing copies unless the conservation of personal data is required under Union Law or member states;

Likewise, according to article 33 of the LOPDGDD, section 3:

> **"3. The person in charge of the treatment will determine whether, when the provision of the services of the person in charge ends, the personal data must be destroyed, returned to the person in charge or delivered, as the case may be, to a new person in charge. The data will not be destroyed when there is a legal provision that requires its conservation, in which case they must be returned to the person responsible, who will guarantee their conservation as long as this obligation persists."**

That is to say, when a person in charge makes an order for the treatment, he must provide in the corresponding contract if, once the provision of the service has been completed, the person in charge must proceed with the deletion or return of the personal data and any existing copies , either to the person in charge or to another person in charge designated by the person in charge.

The destruction will not proceed when there is a legal provision that obliges its conservation, as would be the case with the patient autonomy regulations that establish the conservation of certain medical information of the patient.

In this case, what corresponds, according to the aforementioned regulatory provisions, is for the person in charge to return the data to the person in charge once the task has been completed. It is up to the person in charge (the hospital) to guarantee its preservation while this obligation persists.

Regarding this, the consultation explains that once the laboratory has carried out the analyzes commissioned by the hospitals, the result of them (the personalized results report for each patient) is sent to the hospital electronically or on paper.

When the laboratory sends the results of the ordered analytical tests to the hospital, logically this information is integrated into the patient's HC that the hospital, which is the one who commissioned the test, and who must custody (art. 9.1 Law 21/2000).

The results of the analytical tests, which are integrated into the patient's hospital HC, will be kept as part of this HC which is the responsibility of each hospital, for the time that corresponds to attention to the provisions of the autonomy regulations of the patient

Without prejudice to this, it may be that the person in charge of the treatment, in this case, the laboratory that carried out the analytical test, must keep a copy of the analytical tests carried out with the blocked data, while responsibilities may be derived from the execution of the provision.

Regarding this, according to article 33 of the LOPDGDD, section 4:

> **"4. The person in charge of the treatment will be able to keep, duly blocked, the data as long as responsibilities could arise from their relationship with the person in charge of the treatment."**

In the terms set out in article 33.4 of the LOPDGDD, it would not be contrary to the data protection regulations for the laboratory to keep the data relating to the analyzes carried out, duly blocked, in order to meet, where appropriate, possible responsibilities.

In any case, for the purposes that are of interest in this opinion, the fact that the laboratory must keep blocked certain personal data that it will have processed in care of the hospitals for the time that corresponds according to the patient autonomy regulations, does not distorts the conclusion that, based on the information available, the laboratory would be in charge of the treatment of the different hospitals that subcontract its services.

In relation to the processing contracts that can be entered into between the hospitals and the laboratory, it may be of interest to consult the Guide on the processor in the RGPD prepared by the Data Protection Authorities to help the responsible and those in charge of adapting to the requirements of the RGPD, available on the Authority's website http://apdcat.gencat.cat/ca/inici/.

In accordance with the considerations made in this opinion the following are made,

Conclusions

In the case described in the consultation, the hospital that subcontracts the analysis of its patients to a laboratory, is responsible for the treatment, since it is the one that "determines the purposes and treatment" of the patients' data, and the laboratory is in charge of the treatment of this data.

The fact that the laboratory has to keep blocked certain personal data that it has processed on behalf of the hospitals for the time that corresponds according to the patient autonomy regulations, does not detract from the conclusion that the laboratory is a data controller.

Barcelona, February 13, 2020